System Vulnerability Analysis with the Network Visualization Tool (NVT)[1]

Ronda R. Henning[2]
Kevin L. Fox, Ph.D.[3]

Harris Corporation
Information Systems Division
P.O. Box 98000
Melbourne, FL USA 32902-9800

Summary: For the past 2 years, Harris Corporation has been conducting research for the Air Force Research Laboratory under the Network Visualization Tool (NVT) Program. The NVT concept defines a knowledge solicitation and translation framework for risk assessment. This framework incorporates a graphical description of a network topology, a central repository of modeling data, and report consolidation from multiple risk/vulnerability assessment tools into a single vulnerability assessment. Results are presented to a system user through a comprehensible, graphical interface. The goal of this effort is to investigate the feasibility of developing such a framework for a graphical risk analysis environment that can accommodate both existing and new risk analysis techniques.

The result of the NVT Program is an initial vulnerability visualization and assessment environment, consolidating multi-source output into a cohesive capability with an open, a standards-based architecture. The initial NVT proof-of-concept prototype has been completed. This paper describes the NVT architecture, its components, important architecture features, benefits of the NVT approach, and potential future enhancements.

I. INTRODUCTION

Next generation information systems and infrastructures apply the concept of acceptable risk to vulnerability assessment and coalition information sharing. In this environment, the security features of the system architecture are considered sufficient protection for the mission and any supporting data processed. In previous generations of systems, a risk adverse vulnerability posture dictated custom hardware and software solutions and minimal coalition data interchange. Today, the rapid evolution of technology and the proliferation of computing power mandate the use of commodity Commercial-Off-The-Shelf (COTS) hardware and software components for cost effective solutions. This strong dependence on COTS implies that commercial grade security mechanisms are sufficient for most applications. Security architectures, therefore, must be structured to support building security architectures with relatively weak COTS components. Higher assurance security components are placed at community or information boundaries, forming an enclave-based security architecture that implements a defense-in-depth approach to information assurance.

There are few system architecture design tools available to analyze architecture alternatives. Security risk, system performance, and mission functionality must be balanced while accommodating budgetary constraints. Current generation risk analysis tools usually provide single vendor solutions that address a particular aspects of risk, but are not easily expanded to address emerging technologies and their vulnerabilities. These tools tend to fall into one of three categories:

1. Tools using documented vulnerability databases and possibly repairing known vulnerabilities. Tools of this type are vendor-dependent for database updates, either through new product versions or by a subscription service. Examples of tools in this category are Internet Security System's (ISS) Security Scanner and Network Associates Inc.'s CyberCop.
2. Monolithic tools using various parameters to calculate a risk indicator. These tools are difficult to maintain and harder to keep current in the rapidly evolving threat and technology environment. An example of this tool category is the Los Alamas Vulnerability Assessment Tool (LAVA).
3. Tools examining a particular aspect of the system, such as the operating system or database management system, but ignoring other aspects of the system. SATAN, for example, analyzes operating system vulnerabilities but ignores infrastructure components such as routers and switches.

None of these tools implement an aggregate security snapshot approach to the system, with a "drill down" or layered approach to facilitate addressing risk at various layers (network, platform, database, etc.) of the system. They provide little assistance to system designers when analyzing alternatives among security risk, system performance and mission functionality, instead providing a "risk solution" addressing the particular aspect of risk

1 This research has been entirely funded under the Network Visualization Tool (NVT) program for U.S. AFRL/IFGB, contract #F30602-96-C-0289. U.S. Government Publication Release Authority: Dwayne Allain.

2 Telephone: (407) 984-6009. E-mail: rhenning@harris.com

3 Telephone: (407) 984-6011. E-mail: kfox@harris.com.

EXHIBIT 1

that a given tool was designed to address. To develop a comprehensive risk picture, a tool user would have to become proficient in the use of several tools, and manually correlate the resulting outputs.

Risk analysis is the assessment of the potential system vulnerabilities that may give rise to a security violation. An essential criterion for successful risk analysis is complete and accurate data for the generation of the system models used by the analysis tools. Most of the current risk analysis tools rely on surveys filled out by users, system operations personnel, and analysts to acquire the data for development of the system model. Alternatively, active network scanning may be used to test various vulnerabilities against system components. Textual or survey-based knowledge solicitation techniques are labor intensive and potentially tedious for the analyst. Many of the existing tools reuse the same information to analyze different aspects of the system security.

A centralized repository of system modeling data could provide a basis for shared inputs among existing tools. This repository could generate data sets for use by risk analysis tools, allowing multiple tools to be executed against the same system without separate input activities, and reducing the possibility of operator error. The use of multiple risk tools for backend analysis would allow various aspects of the system to be analyzed without the cost of developing one tool to perform all types of analysis. Integration of the information and the resulting informed assessments made available through multiple tool analyses could produce a more robust and accurate picture of a system's vulnerability posture. By providing an easier framework for alternative evaluation and comparison, these results could facilitate more informed system design decisions.

The Network Visualization Tool (NVT) Program explored the feasibility of defining a shared data repository for risk assessment information. The results of our research included a vulnerability analysis tool framework, a working proof of concept of the architecture, and an innovative application of data fusion technologies to the risk analysis environment. This paper describes the progress and results of the NVT Program.

II. SYSTEM OVERVIEW

Under the Network Visualization Tool program, Harris Corporation defined and developed an innovative and unique vulnerability assessment framework. This framework, the NVT system architecture, can accommodate changes to the threat and the technology environments and preserve the results from current risk analysis tools. The goal of this effort is to research, develop, test, and demonstrate an engineering prototype for a system vulnerability assessment framework that helps system architects identify security vulnerabilities and develop cost-effective countermeasures.

NVT provides a flexible, extensible, and maintainable architecture solution. The NVT prototype isolates factual information about a system from the reporting and processing capabilities of individual vulnerability assessment tools. No single vulnerability assessment tool can adequately address all components of a comprehensive system architecture. A monolithic assessment system is difficult to evolve with the dynamic nature of threat and technology. NVT allows multiple tools to share data and provides a concise, understandable report to the system user. Our objective was to develop a prototype system security engineering tool that:

- Functions as a design tool to identify vulnerabilities in an architecture before the architecture is built and help enforce good security design principles
- "Snapshots" a system and its vulnerabilities, and compares how risk evolves over the system life cycle
- Applies static vulnerability databases from a variety of sources
- Applies legacy risk analysis tools and threat models
- Correlates information from various risk models/tools into a more comprehensible picture of the system's vulnerabilities
- Allows what-if analysis to facilitate comparative analysis among security, functionality, performance, and availability
- Provides an easy to use capability to specify the security relevant characteristics of a system design
- Our vision of a system security engineering tool that facilitates system vulnerability assessment incorporates a single, graphical representation of a system. This system representation is provided to multiple risk/vulnerability assessment tools and vulnerability data or knowledge bases, resulting in a single source, consolidated input system model for multiple tools. The NVT prototype integrates and interactively applies multiple existing risk assessment technologies. A Fuzzy Expert System applies the unique correlation technology of ***FuzzyFusion***™ to combine the results from the various tools into a single, clear, cohesive vulnerability assessment report. The concept is illustrated in Figure

The NVT prototype is implemented on an Intel Pentium PC platform running Windows NT. This platform was selected as a low cost solution supporting a large variety of assessment tools. The initial tool suite employs a number of COTS/GOTS capabilities including:

- HP OpenView, for network automatic discovery or manual network modeling.
- ANSSR, a Government-Off-The-Shelf (GOTS) network system analysis tool developed by MITRE.
- RAM, NSA's risk assessment methodology, implemented in the DPL-F decision support programming language.
- Internet Security Systems Internet Scanner, a scanning vulnerability tool suite.

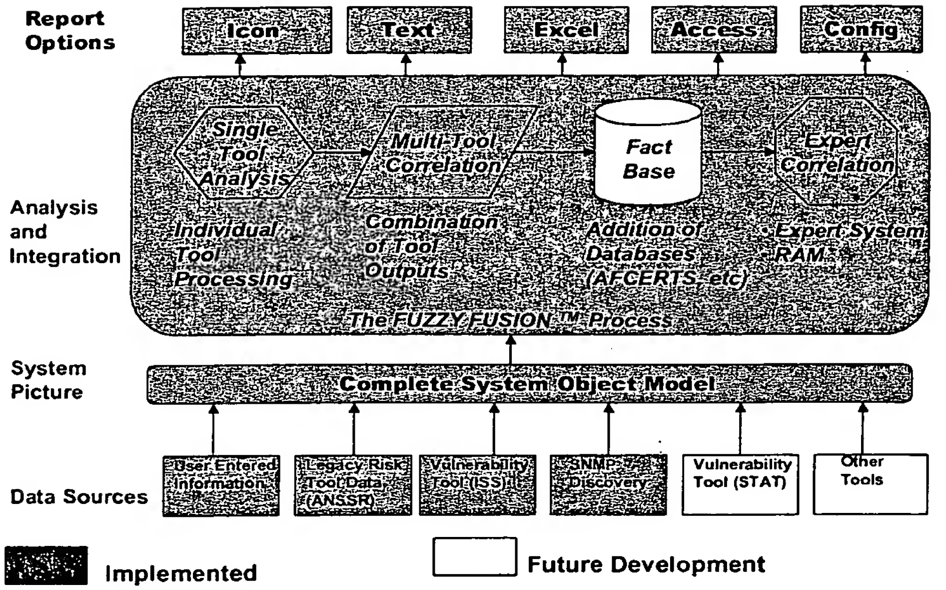

Figure 1. – The NVT Vulnerability Assessment Tool Architecture Concept.

II.1 System Architecture Data Entry

NVT is based on the concept of a knowledge solicitation framework that incorporates a graphical description of a network topology. This topology is used for capture of network attributes, and is subsequently analyzed for security vulnerabilities. The knowledge solicitation portion of NVT applies modern network discovery capabilities and a graphical user interface. This improves the accuracy of the network model, provides a common network description for multiple risk analysis reasoning engines, and enhances the productivity of the system security analyst.

The NVT prototype automatically maps an existing network, or can be used for the manual entry of a network design. The prototype uses HP OpenView to graphically depict a network topology. As illustrated in Figure 2, once it has been given the IP address of the default router for the network, NVT, through the use of OpenView, can search for computers and other devices attached to the network. It performs an active search, pinging possible IP addresses on the network, and adding whatever response information it receives to its network map. NVT also provides, through OpenView, a manual method to draw a proposed network with a graphical user interface that supports drag and drop, as illustrated in Figure 3.

Through this interface, a System Security Engineer can rapidly define a given system architecture, including the security critical information. For example:

- A user can apply the manual entry capability to consider alternative designs as part of a trade study.
- A user may edit the properties of each node, providing additional details as required to provide complete logical network planning.
- A user can also represent an entire network on a map by using a subnetwork icon. A detailed map of the subnetwork can be linked to this icon and displayed by double clicking on the icon.

Once the system description has been completed, the NVT prototype represents and stores the description in an object/class hierarchy. This single topological model supports the information needs of multiple vulnerability assessment tools, as well as the ***FuzzyFusion***^{TM} of their results into a cohesive risk assessment. NVT translates this system representation into the appropriate format for each of the assessment tools employed. This single object representation of the system simplifies the use of multiple tools, eliminating redundant data entry. It also provides the foundation for addressing the problem of incomplete data for a given vulnerability assessment tool, and for future knowledge negotiation capabilities to correct data inconsistencies.

II.2 Risk Analysis Tool Selection

Under the NVT Program, Harris surveyed current COTS, GOTS and research vulnerability assessment and reasoning tools to determine their capabilities and availability. Tools were categorized by the types of vulnerabilities assessed, and their functional characteristics. Each tool was further evaluated on its data acquisition and output formats to determine how the information can be applied in the NVT engineering prototype implementation. The primary criteria were the operating system required by the tool, the capability of the tool to assess network environments, the data gathering methods used by the tool, and the risk types assessed by the tool. The vulnerability assessment and reasoning tools selected had to be able to execute in the NVT prototype's operational environment (a PC with Windows NT).

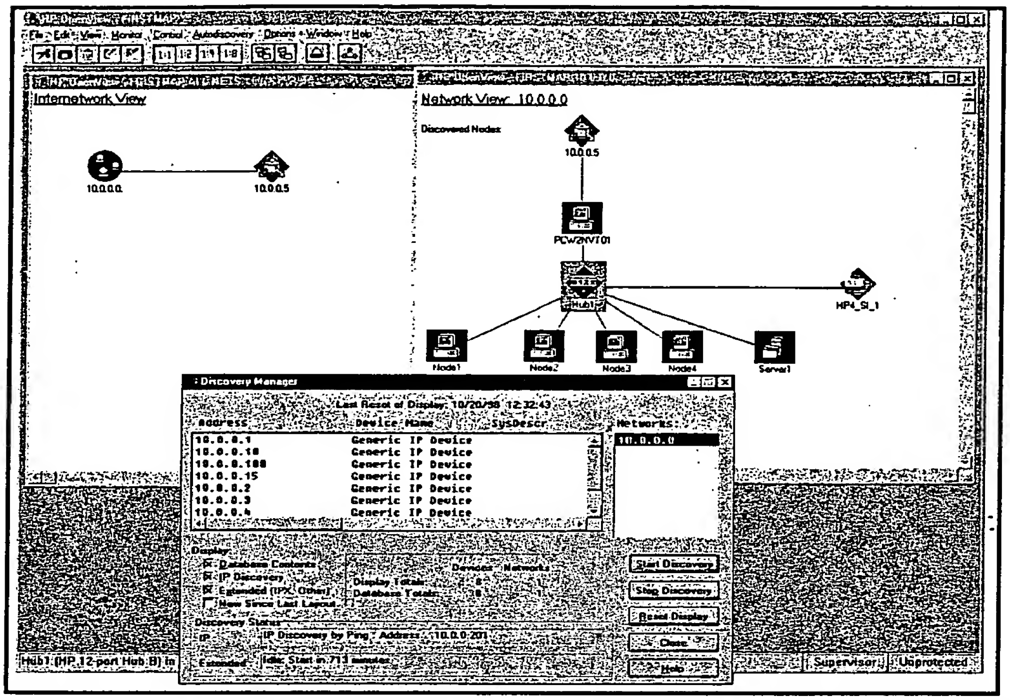

Figure 2. HP OpenView's Network Discovery Tools enable NVT users to map an Existing Network for Further Security Analysis

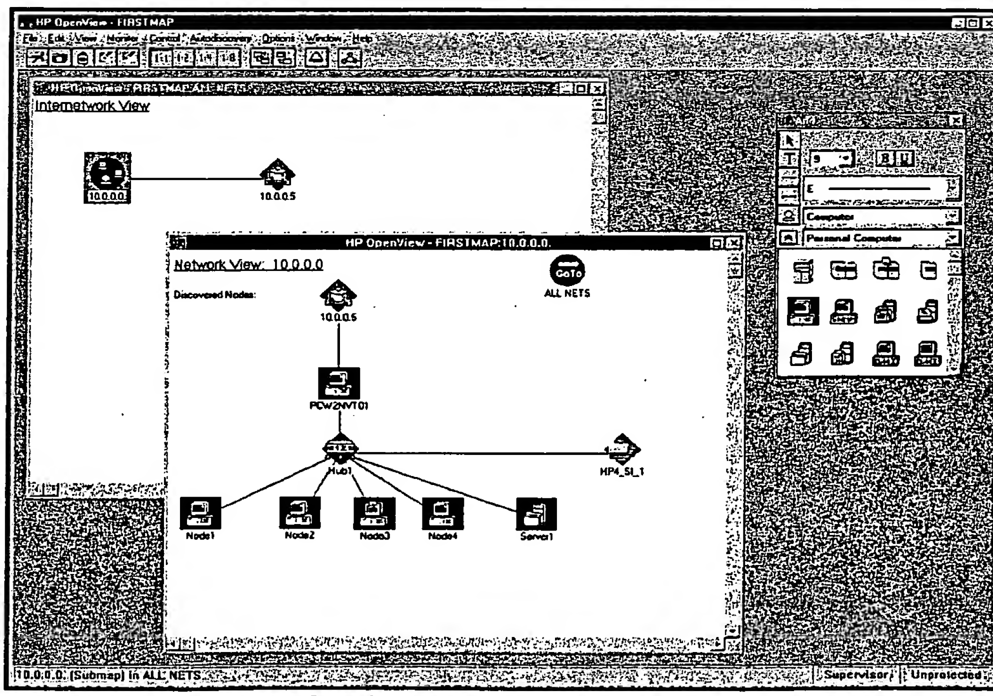

Figure 3. OpenView's Manual Entry Capability is used to provide NVT users with a Mechanism to Consider Alternative Designs as Part of a Trade Study

A primary purpose of the NVT prototype was the demonstration of a framework with the flexibility to integrate and interactively use multiple existing vulnerability assessment and reasoning technologies. In order to demonstrate the proof of concept of integrating and interactively using multiple existing vulnerability assessment and reasoning technologies within program restrictions, a representative sample of tools was selected for inclusion in NVT. As a result of the tool survey, ANSSR, RAM, and ISS Internet Scanner were selected for inclusion in NVT. These three tools met the project requirements and provided the greatest diversity of func-

tional capabilities, as shown in Table 1, The Selected Tools' Capabilities Summary. The selected tools represented the greatest diversity of reasoning characteristics with the lowest number of expected integration risks.

The MITRE Corporation's Analysis of Networked Systems Security Risks (ANSSR) prototype is a risk analysis tool which simulates attacks on information systems and communications between them that result in unauthorized disclosure of sensitive information. These simulated attacks, or threat scenarios, can be initiated by different types of attackers, including insider threats as well as those coming from outside an intranetwork . ANSSR compares the risk-reducing effects of different sets of safeguards in light of a given security concept of operations. Safeguards include computer security (COMPUSEC) features and assurances, communications security (COMSEC) controls, emanations protection, physical security, and procedural controls. ANSSR explicitly analyzes risks due to networking. ANSSR 2.2 includes simulated passive and active wiretap attacks as well as attacks in which an attacker, logged on at one system, exploits that system's connectivity to other systems to attack them. ANSSR can also be applied to a stand-alone system. An analyst can enter or reuse a baseline system description, then ask ANSSR to develop all possible scenarios against the baseline system. Single-scenario risks are aggregated into a bottom-line risk of all possible scenarios. ANSSR is intended primarily for use during the requirements definition phase, but can also be used to guide the risk analysis performed to support accreditation.

Internet Security Systems' (ISS) Internet Scanner is a fast, comprehensive and proactive Windows NT and UNIX network security scanner. It is a vulnerability assessment product that analyzes the security of devices on an enterprise-wide network. It has 30 predefined reports that are used to collect the information needed to make security policy decisions. Internet Scanner performs a variety of vulnerability detection, ranging from information-gleaning exercises to finding vulnerabilities. It finds vulnerabilities much as an intruder would – by examining a network's devices, services, and interrelationships. Internet Scanner provides detailed information about all vulnerabilities detected, including the vulnerable host, description, and corrective actions. It also provides illustrated management and trends analysis reports. Internet Scanner can be used on all TCP/IP-based networks – networks connected to the Internet as well as stand-alone networks and machines.

NSA's Risk Analysis Model (RAM) is a methodology to help balance an acceptable risk profile. RAM is a flexible methodology, utilizing event trees and a functional probabilistic decomposition of a problem. It moves the risk assessment process from a qualitative discipline to quantitative discipline. Users identify the probabilities of various events, and RAM aggregates the probabilities, as well as addressing vulnerabilities over time. RAM is an analytic methodology that enables analysis of risk for decision trade-offs. It allows for sensitivity analysis, and identifies the weakest links of a system. RAM has been incorporated into a COTS tool, the DPL-f programming language for decision support, developed by Applied Decision Analysis LLC, a wholly owned subsidiary of Price Waterhouse Coopers Ltd.

DPL (Decision Programming Language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into the decision process. DPL provides a graphical interface for building a model, and performs a variety of analyses on the model. DPL-f contains all of the functionality built into DPL. In addition, DPL-f provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f contains some unique analytic tools as well. These include the ability to calculate explicitly the probability of any event in the tree and to perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows the modeler to account for devaluation, capital

Table 1. The Selected Tools' Capabilities Summary

Selected Tool	Functional Capabilities	
ANSSR (Analysis of Networked Systems Security Risks) MITRE Corporation	*Passive data gathering* - Model structure - Survey based data gathering - Network aware	*Risk Type* - Single Occurrence of Loss
RAM (Risk Assessment Model) NSA	*Passive data gathering* - Event tree - Prioritized attack list *Risk Type* - Mathematical model - Multiple risks/services - Event based over time	*Extensible to Risk Type* - Comparison of effectiveness of different designs - Not limited to computers/networks - Optimization of system/cost benefit analysis
ISS Internet Scanner Internet Security Systems (ISS) Corporation	*Active data gathering* - Scans network for hosts, servers, firewalls, and routers - Assesses security and policy compliance of networks, operating systems, and software applications	*Risk Type* - Computer Network Compliance Report (snapshot in time)

growth, or other time-varying quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets, and a graphical portrayal of risk over time.

II.3 Output Report Correlation and Generation

None of the above tools take an aggregate snapshot approach to the system, with a "drill down" or layered approach to address risk at various layers (network, platform, database, etc.) of the system. Using multiple risk analysis tools would allow various aspects of the system to be analyzed for vulnerabilities without the cost of developing one tool to perform all types of analysis. To provide a more comprehensive vulnerability assessment of a system than any one tool could provide, the outputs of the various tools must be integrated and fused into a single, concise report. This provides greater assistance to system designers analyzing alternatives among security risk, system performance, and mission functionality.

Under the NVT effort, Harris investigated technologies that would support our goal of integrating and fusing the results from multiple vulnerability analysis applications. By examining the variety of current COTS and GOTS products, and the variety of inputs and outputs those products require, it became apparent that fuzzy decision technology offered the most flexible solution to our problem. Our focus on fuzzy decision methodologies as our technological foundation was based on an analysis of a variety of technologies, including Expert Systems, Databases Systems, Neural Networks, Fuzzy Logic, and Fuzzy Expert Systems. Fuzzy Expert Systems are based on the premise that multi-criteria, multi-expert decision making can lead to a best-fit answer. The primary benefit of a fuzzy reasoning system is its ability to use and assimilate knowledge from multiple sources. We believe that Fuzzy Expert System technology is most applicable to the NVT architecture because:

- At least one expert exists for each tool that we wish to include in the system
- The problem itself is fuzzy; it has ambiguities and often partial information
- We can incrementally learn and apply new technologies as the system grows
- We believe we can identify valid membership functions for the mapping of data to concept and concept to knowledge

NVT performs *FuzzyFusion™* to combine the results of multiple vulnerability assessment/risk analysis tools into a unified report. The *FuzzyFusion™* is accomplished through the use of a Fuzzy Expert System, which combines the outputs of the various tools, user concerns about system risks and vulnerabilities, and expert understanding of the results of each tool and how these fit into the larger information system security picture.

Output of the concise assessment can be provided to the NVT user through multiple means and in various degrees of detail, as illustrated in Figure 4. The graphical network map of a system can be color-coded to provide a visual indication of where the greatest risks are located. In Figure 5, the node with the greatest associated risk is colored red. Less severe risks are colored yellow. A pop-up slider window can also be used to indicate the top *N* risks, and their severity. Further details, such as text reports and spreadsheet analyses, can be accessed by drilling down through the layers of information.

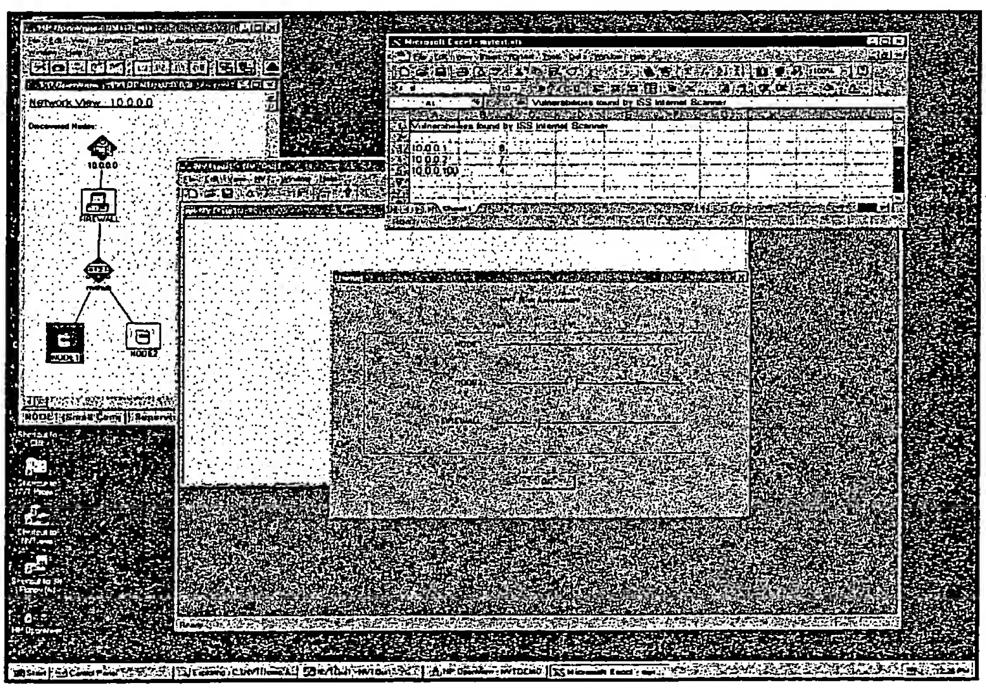

Figure 4. NVT leverages Existing Vulnerability Assessment Tools to present a Single Cohesive Risk Picture

III. FEATURES AND BENEFITS OF NVT

The result of the NVT Program is a prototype demonstrating a comprehensive vulnerability profile based on the user's defined acceptable risk of compromise to a given system. End users have a simple expression of the *vulnerability posture* of a given system or system design, and are capable of performing *"what if"* analysis for functionality, performance, and countermeasure trades.

The primary advantage of the NVT prototype is that it provides a flexible, modular, extensible approach to vulnerability assessment. This innovative design accommodates multiple risk assessment techniques, but only requires single entry of the system description (through auto discovery or manual entry of a model), which is a significant benefit to the System Security Engineer. Figure 5 illustrates the NVT interface to ANSSR. In stand-alone use, ANSSR uses a character based GUI for user data input. As the number of windows and menus suggests, entry of information into the tool is a manually intensive exercise. One of the benefits of NVT is that it automatically provides the required system information to the various vulnerability assessment tools, allowing each tool to use only the input data it requires. NVT eliminates the labor-intensive methods associated with using the legacy assessment tools while preserving the existing user investment in legacy methodologies. NVT also provides a mechanism to correlate information among several tools. Information solicited from the user for any single tool is shared among all tools. Legacy vulnerability assessment tools and databases can be reused, and their results used in conjunction with alternate risk models.

NVT was designed to be an affordable vulnerability assessment environment. Many monolithic risk assessment tools require high performance Unix platforms and cost over $40,000 per copy. The NVT prototype was developed on a Windows NT-based Pentium platform. Our initial tool suite reflects a desire to be economical and pragmatic in tool selection. Three COTS/GOTS vulnerability assessment tools are incorporated into the framework: ANSSR, RAM, and ISS Internet Scanner. Costs for the runtime licenses of COTS products currently employed within the NVT prototype along with a suitable NT workstation are approximately $12,000.

The modular, extensible system design for NVT ensures ease of technology transition and integration as new vulnerability tools and technology vulnerabilities come to market. Our estimate for the incorporation of new tools into the NVT environment is approximately eighty hours of engineering integration. This modularity preserves user legacy models and tool investments, allowing each user to select the tools most appropriate for his environment and needs.

IV. COMPARISON WITH OTHER WORK

To the best of our knowledge, no current risk assessment tool environment is designed as an *integrable architecture*. Most tools on the market today either perform real time, active scanning analysis of a single node within a network, or ask for user input on the network system and its physical environment. Each of these

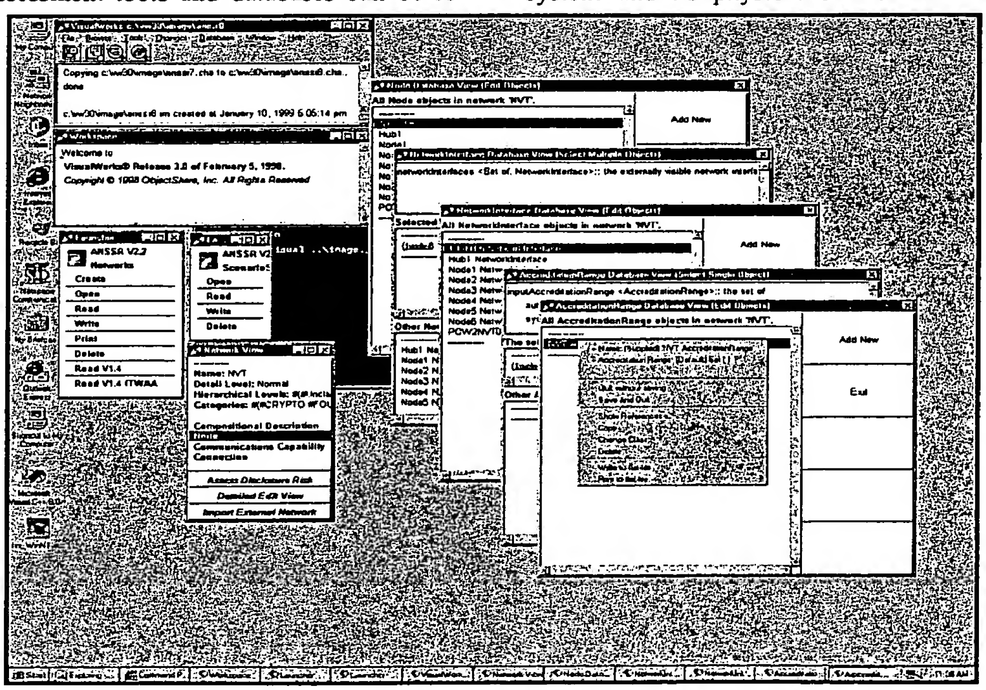

Figure 5. Entering System Information into the Interface for ANSSR is a Manually Intensive Process

techniques is valuable for a particular class of problems. However, the ability to accommodate new protocols, vulnerabilities, and classes of devices within a single risk assessment framework is extremely valuable. NVT also provides a comprehensive graphical output capability that consolidates multiple tool outputs into a cohesive system risk profile. NVT was designed to make risk assessment a feasible, comprehensible activity without requiring the user to develop comprehensive expertise in the interpretation of risk analysis results.

The only tool suite that is as ambitious as NVT is CRAMM, the Central Computer and Telecommunications Agency's (CCTA) Risk Analysis Management Methodology. CRAMM allows security assessments to be conducted in terms of security objectives (policy statements), security functions (countermeasures), or security examples (implementations). CRAMM is designed to be a comprehensive risk assessment system. As such, it is not designed for casual users, but for trained risk analysis experts with a high degree of expertise in the use and interpretation of CRAMM results.

V. FUTURE RESEARCH

The basic foundation of NVT provided valuable experience in risk analysis tool integration and correlation technologies. Future research and development efforts will benefit from the use of the NVT prototype by System Security Engineers. These uses will include applying NVT to:

- Identify vulnerabilities and enforce good security design principles
- "Snapshot" a system and its vulnerabilities, and compare how risk evolves over the system lifecycle
- Correlate information from various risk tools in an understandable graphical vulnerability analysis
- Support hypothetical analysis, facilitating architecture choices among security, functionality, performance, and availability
- Provide rapid specification of the relevant characteristics of a system design

Beyond the efforts conducted under the initial NVT Program, further research is need to improve the ***Fuzzy-Fusion***™ used to combine outputs from various risk analysis tools into a unified report. In addition, we have identified new functionality to incorporate into the results analysis, including:

- **Temporal Based Reasoning**. Accounts for the time required to exploit a known vulnerability as part of the system assessment process. It enables an analyst to perform a vulnerability assessment that accommodates the time required to exercise a given vulnerability. For example, if the time that is required to compromise a given node is greater than the timeline for mission completion, then the threat is minimal.
- **Vulnerability Thresholding**. Minimizes continued computation when an aggregate vulnerability level in a given system or segment exceeds a user defined limit, allowing the user to define his own vulnerability tolerance. It eliminates possibly computationally intensive search trees when a sufficiently lethal vulnerability is located, or when a large number of vulnerabilities are identified. It allows the user to define his vulnerability tolerance level and supports configurable definitions of acceptable levels of vulnerability.
- **Reasoning with uncertainty or incomplete data information**. Provides the user with some answer, usually the best solution that is available with the information available at a given moment in time.
- **Vulnerability trade-off visualization techniques**. Allow the user to easily perform what-if analysis and experimentation among performance, functionality, and countermeasures. It enables the user to readily understand the possible comparisons among desired capabilities.

This functionality will allow NVT to more accurately reflect the human decision making process. Further, it will support a more robust, systems orientation towards vulnerability analysis, accommodating consideration of application and platform vulnerabilities as well as conventional network vulnerabilities.

VI. REFERENCES

- "Comparison of COTS Network Management Tools For Knowledge Solicitation". Network Visualization Tool Program – Task 1 Report. Harris Corporation. Melbourne, Florida. September 1997
- "Comparison of COTS Vulnerability Assessment/Reasoning Engines for Automated Reasoning". Network Visualization Tool – Task 3 Report. Harris Corporation. Melbourne, Florida. October 1998.
- "A Practitioner's View of CRAMM". Norman Truman. Gamma Secure Systems Limited. http://www.gammass1.co.uk/topics/hot5.html. September 1997.
- "Sniffing Out Network Holes". Leslie O'Neil and Joe Scambray. *INFOWORLD*. February 8, 1999. Pp. 74-82.
- "L-3 Network Security Expert 3.0". Product review, *SC Magazine* (Information Security News). http://www.infosecnews.com/13/13.html.
- *Analysis of Networked Systems Security Risks (ANSSR) Assessment Tool, Version 2.2, User's Manual*. D. J. Bodeau and F. N. Chase. The MITRE Corporation. Bedford, MA.
- "ANSSR: A Tool for Risk Analysis of Networked Systems". D. J. Bodeau, F. N. Chase, and S. G. Kass. *Proceedings of the 13th National Computer Security Conference*. October 1990.
- *DPLf User Manual*. Applied Decision Analysis LLC. 1999.
- *ISS Internet Scanner User Guide for Windows NT*. Internet Security Systems (ISS). Atlanta, GA. 1997.

- *HP OpenView for Windows: Workgroup Node Manager User's Guide*. Hewlett Packard. Cupertino, CA. 1998.
- *HP OpenView: Professional Suite Getting Started Guide*. Hewlett Packard. Cupertino, CA. 1998.